Microsoft Security

LES 4 SAISONS DE LA data
IA • CYBERSECURITÉ • PROTECTION DES DONNÉES

Renforcer sa stratégie de protection des données à l'ère de l'IA : bonnes pratiques techniques & juridiques

jeudi 3 juillet 2025, 15h15 – 15h45

Marina Djouadi
Spécialiste Technique, protection des données
Microsoft

Paul Perrin
Responsable Juridique
Microsoft

Renforcer sa stratégie de protection des données à l'ère de l'IA

- Enjeux juridiques de l'IA : les perspectives de Microsoft
- IA & données : garder la main grâce à *Data Security Posture Management (DSPM) for AI*

Enjeux juridiques de l’IA : les perspectives de Microsoft

Microsoft's existing privacy commitments apply to AI

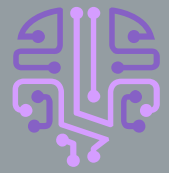
We will keep your organization’s data private

You are in control of your organization’s data

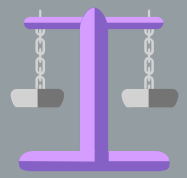
Your access control and enterprise policies are maintained

Your organization’s data is not shared

Your organization’s data security and privacy are protected by design



Your organization’s data is not used to train foundation models without your permission



Our products and solutions comply with global data protection regulations.

IA & données

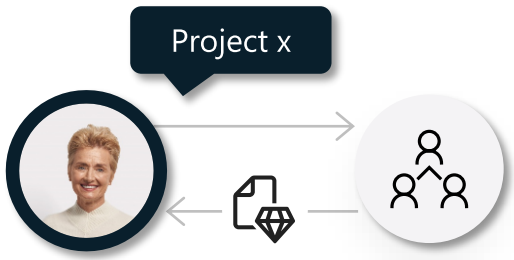
Garder la main grâce à DSPM for AI

Les défis de la GenAI

1

Partage excessif de données

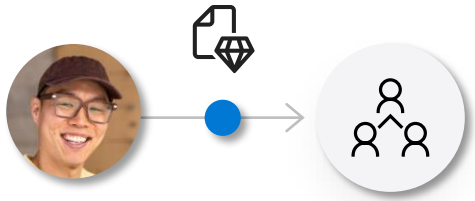
Les utilisateurs peuvent accéder à des données sensibles via des applications d'IA sans autorisation appropriée



2

Fuite de données

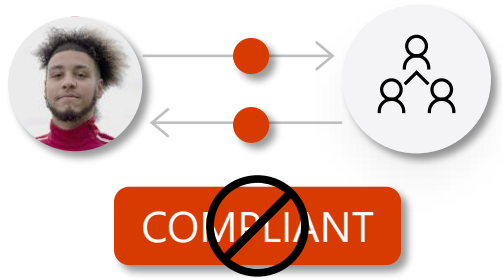
Les utilisateurs peuvent divulguer par inadvertance des données sensibles à des applications d'IA



3

Utilisation non conforme

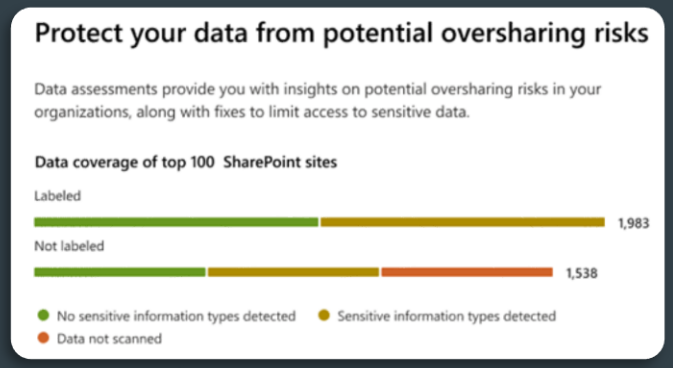
Les utilisateurs peuvent recourir à des applications d'IA pour générer du contenu contraire à l'éthique ou à haut risque



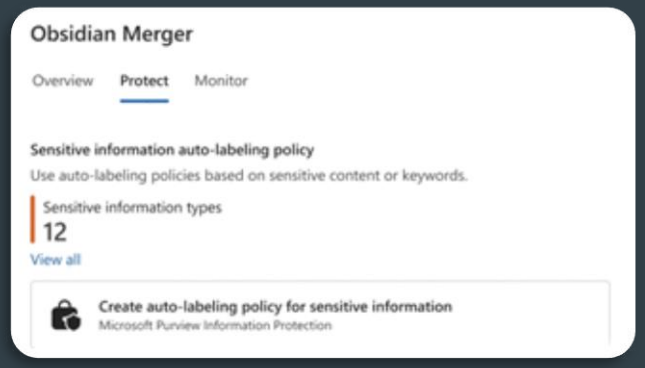
Identifier et réduire les risques liés à l'utilisation de l'IA

Data Security Posture Management (DSPM) for IA

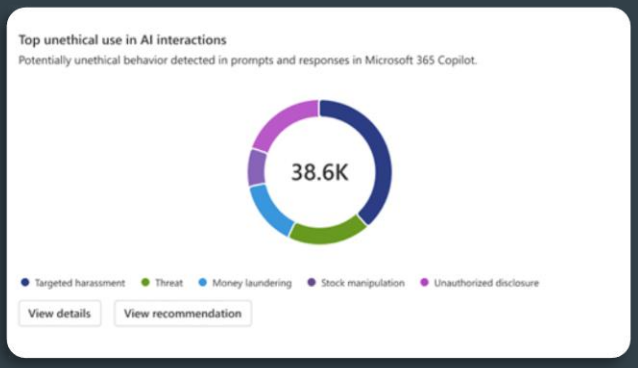
Renforcez de manière proactive la sécurité des données pour prévenir les incidents tels que le partage excessif, les fuites ou l'utilisation non conforme des données



Découvrez les risques liés à la sécurité, et à la conformité des données dans les rapports, et les revues de vos espaces de partage

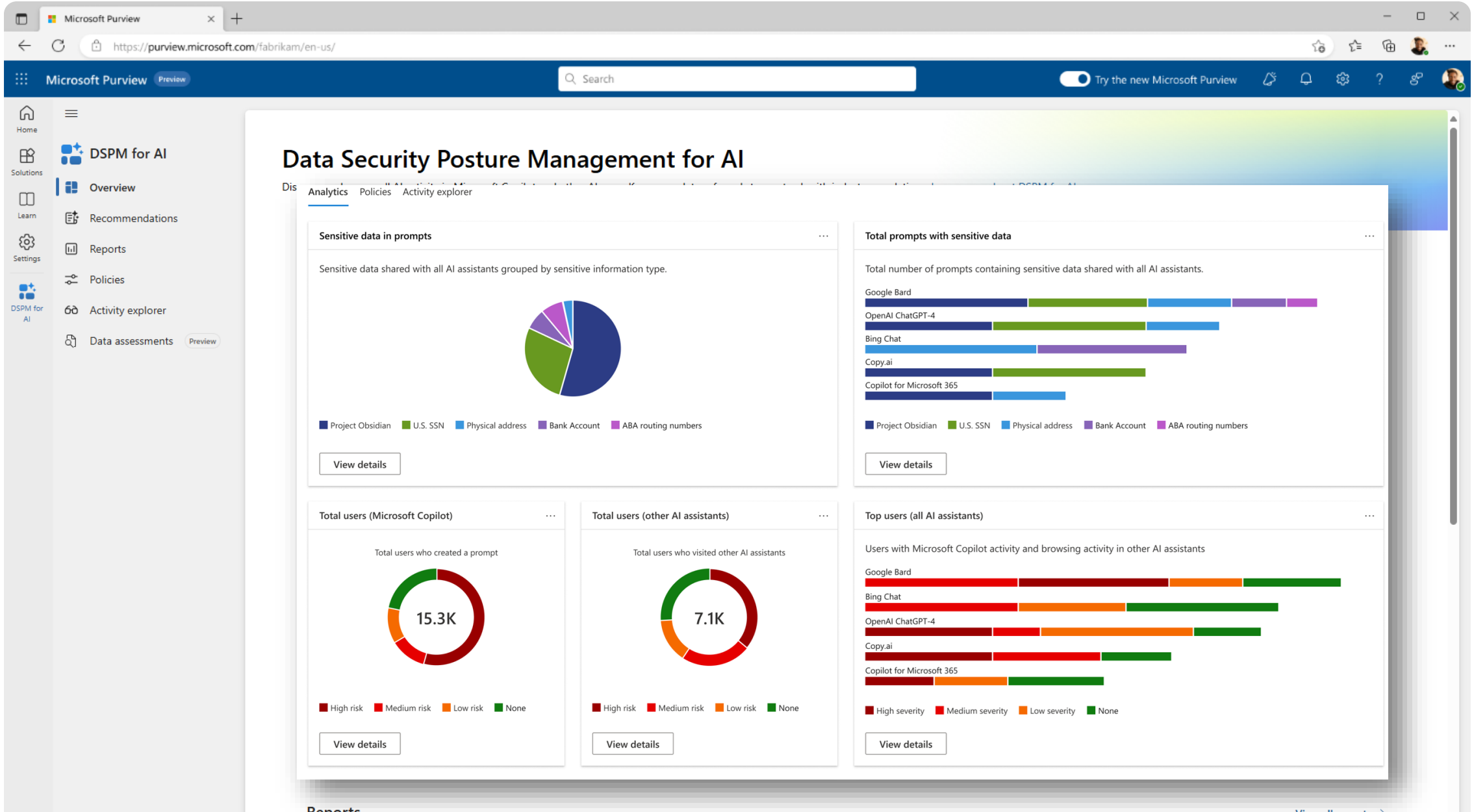


Protégez les données sensibles contre la surexposition grâce à des recommandations et une application, en un clic, d'étiquettes de confidentialité

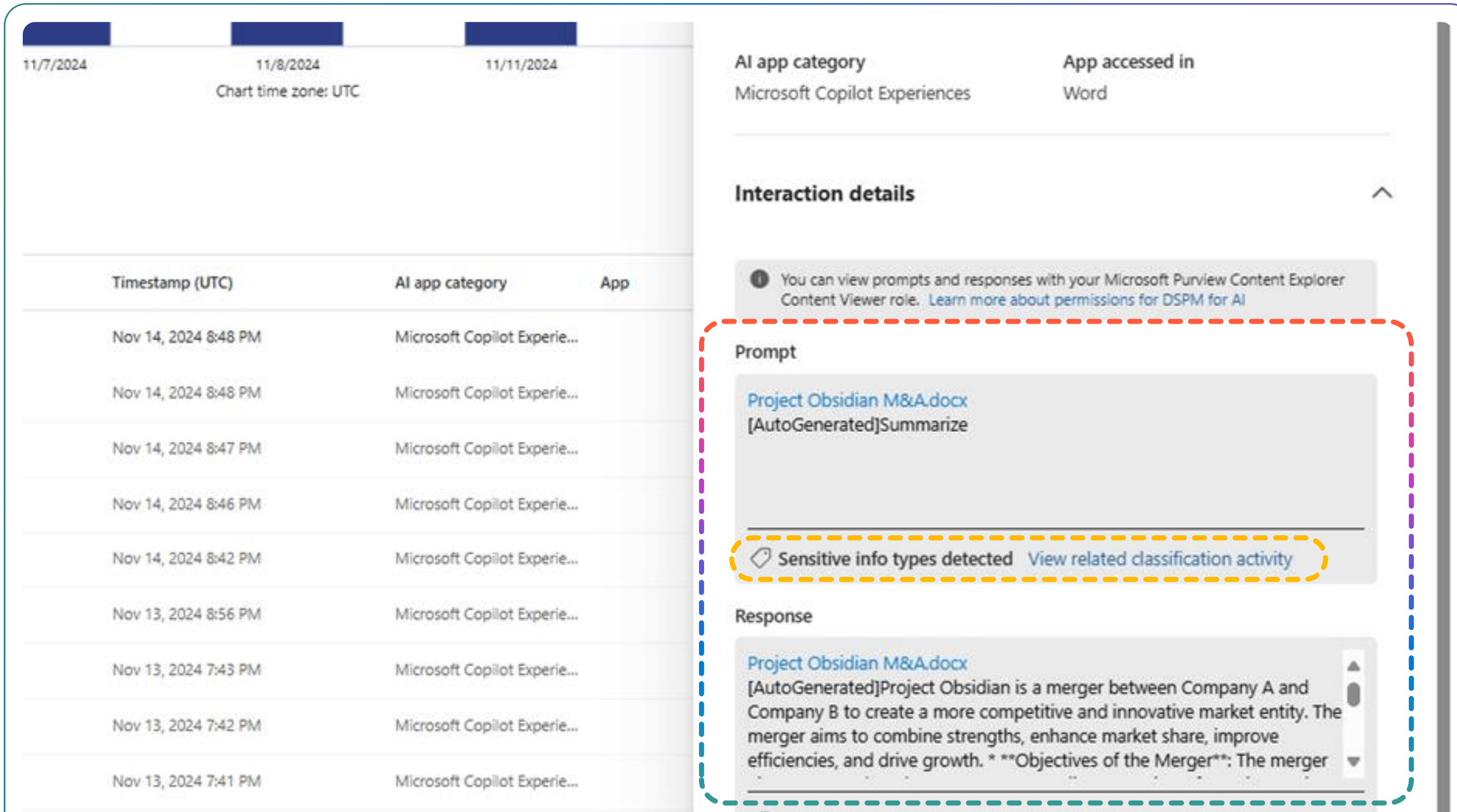


Superviser l'utilisation de l'IA en cas d'usage non conforme et obtenir des recommandations sur l'application des politiques de conformité

Data Security Posture Management for AI



Data Security Posture Management for AI



Gagnez en visibilité sur le contenu surpartagé

Identifier les partages potentiellement excessifs
Sites et fichiers

Sites et fichiers contenant des données sensibles

Données partagées à grande échelle

Données fréquemment consultées

Prioriser les risques les plus élevés

Évaluation du risque

Risque élevé

Risque moyen

Risque faible

Exemple

Un site contient des documents avec des numéros de carte de crédit

+

Tous les membres de l'organisation peuvent accéder au contenu du site

+

575 utilisateurs ont accédé au contenu du site la semaine dernière

=

Risque élevé : Prioriser l'assainissement

Home
Solutions
Learn
Settings
Data Lifecycle Managem...
eDiscovery
Data Loss Prevention
DSPM for AI
Insider Risk Managem...

DSPM for AI
Overview
Recommendations
Reports
Policies
Activity explorer
Data assessments Preview

Data assessments (preview)

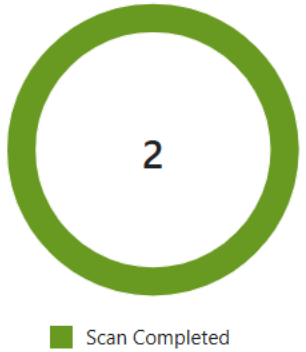
Identify oversharing risks

Use data assessments to identify potential oversharing risks in your organization. They also provide fixes to limit access to sensitive data.

Assess and prevent oversharing

1. **Create an assessment**
   Choose the data sources and users you want to assess.
2. **Evaluate data**
   Review the assessment scan results for users who overshare data from the data sources.
3. **Apply fixes**
   Limit Microsoft Copilot access to sensitive data, apply label and retention policies to sites and data. Conduct site and access reviews to evaluate permissions and user access.

Assessment status



Oversharing Assessment for the week of December 2, 2024

Default data assessments scans the top 100 sites in your organization

Sensitivity labels on data of top 100 sites

Labeled
4.3k

Not labeled
59.1k

No Sensitive Information Types Detected 2 more

+ Create assessment

2 items Group

Assessment name	Status	Scan started on
Default assessments (2)		
Oversharing Assessment for the week of December 2, 2024	Scan completed	Dec 6, 2024 1:34
Oversharing Assessment for the week of November 18, 2024	Scan completed	Nov 20, 2024 10:

Home
Solutions
Learn
Settings
eDiscovery
Data Loss Prevention
DSPM for AI
Insider Risk Managem...
Information Protection

Oversharing Assessment for the week of November 18, 2024

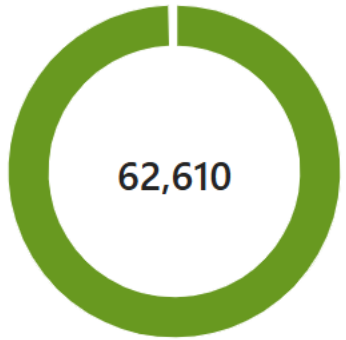
Assessment info

Description
Default assessment created by Purview

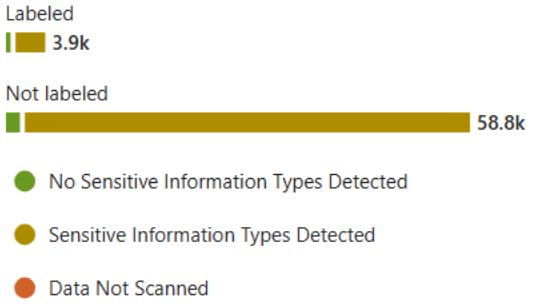
Total items
62,610

Sources included
66

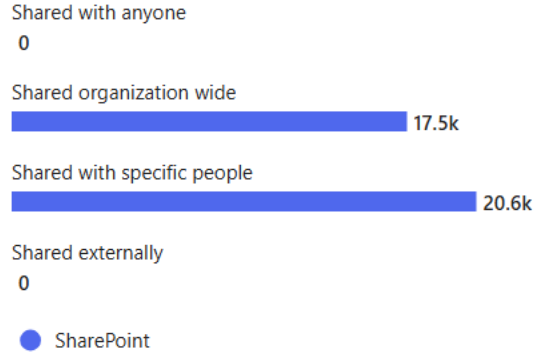
Total items



Sensitivity labels on data



Data with sharing links



66 items Group

Data source ID	Source type	Total items	Total items acces...	Times users a...	Unique users acc...	Total sensitive ite...	Total scanned ite...	Total unscanned ...	Sharing
/sites/obsidianmerger/	SharePoint	3,845	15	60	2	3,838	3,845	0	Specif
/sites/finance/	SharePoint	6,980	26	53	2	6,725	6,980	0	Organ
https://p4aidemo-my.sharepoint.com/	SharePoint	Coming soon	12	29	3	Coming soon	Coming soon	Coming soon	Comir

Home
Solutions
Learn
Settings
eDiscovery
Data Loss Prevention
DSPM for AI
Insider Risk Managem...
Information Protection

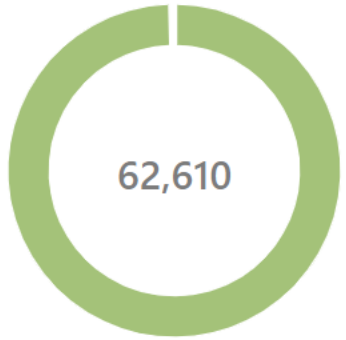
Assessment info

Description
Default assessment created by Purview

Total items
62,610

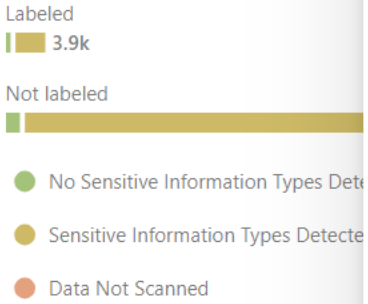
Sources included
66

Total items



Scanned For Sensitive Info Types
Not Scanned

Sensitivity labels on data



Data source ID	Source type	Total items ↓	Total items acces...	Times users ac
/sites/finance/	SharePoint	6,980	26	53
/sites/samplefiles/	SharePoint	6,874	0	0
/sites/financeweb/	SharePoint	6,859	0	0
/sites/delivery/	SharePoint	6,842	0	0
/sites/asia/	SharePoint	6,751	0	0

/sites/finance/

Overview | Protect | Monitor

Data source details

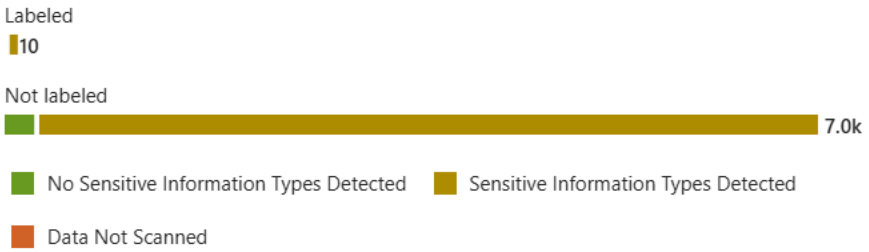
Data source type
SharePoint

URL
https://p4aidemo.sharepoint.com/sites/finance/

Data coverage

Total items in site
6,980

View items



Home
Solutions
Learn
Settings
eDiscovery
Data Loss Prevention
DSPM for AI
Insider Risk Managem...
Information Protection

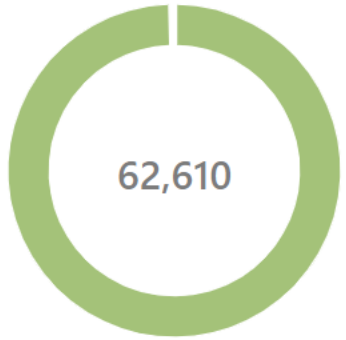
Assessment info

Description
Default assessment created by Purview

Total items
62,610

Sources included
66

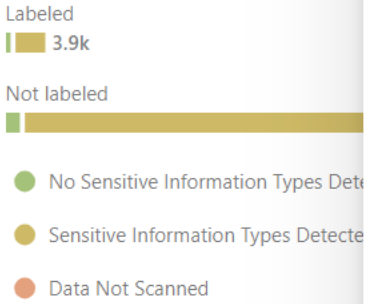
Total items



Scanned For Sensitive Info Types

Not Scanned

Sensitivity labels on data



Data source ID	Source type	Total items ↓	Total items acces...	Times users ac
/sites/finance/	SharePoint	6,980	26	53
/sites/samplefiles/	SharePoint	6,874	0	0
/sites/financeweb/	SharePoint	6,859	0	0
/sites/delivery/	SharePoint	6,842	0	0
/sites/asia/	SharePoint	6,751	0	0

/sites/finance/

Overview | **Protect** | Monitor

Limit Microsoft 365 Copilot access to this site

Choose how you would like Copilot to access data in this SharePoint site.

Restrict access by label
Microsoft Purview Data Loss Prevention

Restrict all items
SharePoint Restricted Content Discoverability

SharePoint Administrators or Global Administrators can enable Restricted Content Discoverability in SharePoint Online in your organization.

Steps at a glance

1. **Download and install SharePoint Online Management Shell.** Download the latest version of SharePoint Online Management Shell
2. **Connect to SharePoint Online as a Global Administrator or SharePoint Administrator in Microsoft 365.** To learn how, see Getting started with SharePoint Online Management Shell
3. **Apply Restricted Content Discoverability on a SharePoint site.** Run the following command in SharePoint Online Management Shell:

```
Set-SPOSite -identity <site-url>
-RestrictContentOrgWideSearch $true
```

4. **View the Restricted Content Discoverability configuration for a given site.** Run the following command in SharePoint Online Management Shell:

```
Get-SPOSite -identity <site-url> | Select
RestrictContentOrgWideSearch
```

Other labeling policies

Default sensitivity label for SharePoint document library

Home
Solutions
Learn
Settings
Data Lifecycle Managem...
eDiscovery
Data Loss Prevention
DSPM for AI
Insider Risk Managem...

DSPM for AI
Overview
Recommendations
Reports
Policies
Activity explorer
Data assessments Preview

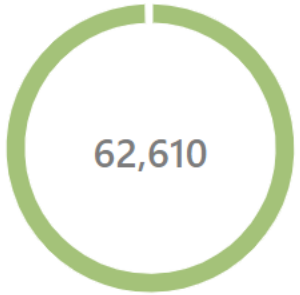
Assessment info

Description
Default assessment created by Purview

Total items
62,610

Sources included
66

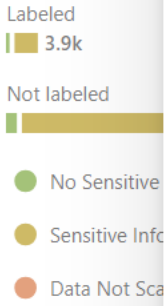
Total items



Scanned For Sensitive Info Types

Not Scanned

Sensitivity lal



Data source ID	Source type	Total items ↓	To
/sites/finance/	SharePoint	6,980	2
/sites/samplefiles/	SharePoint	6,874	0
/sites/financeweb/	SharePoint	6,859	0
/sites/delivery/	SharePoint	6,842	0
/sites/asia/	SharePoint	6,751	0

/sites/finance/

Other labeling policies

Default sensitivity label for SharePoint document library

When a default sensitivity label is created, the label will only apply to new items added to the site. Select a sensitivity label in the SharePoint site.

Create default sensitivity label for SharePoint document library
Microsoft SharePoint location

Default labels

Label all new items by default using sensitivity labels. The admin can define labels with protetion and labels with no protection. Assign default labels when creating a label policy.

Assign default sensitivity label
Microsoft Purview Information Protection

Sensitive information auto-labeling policy

Files with sensitive info types
6,725

View items

Use auto-labeling policies based on sensitive content or keywords.

Create auto-labeling policy for sensitive information
Microsoft Purview Information Protection

SharePoint site sensitivity label

This label will only apply to the site and not the contents of the site.

Apply a sensitivity container label to the site.

Sécurisez et gouvernez les données pour une utilisation responsable de l'IA

Sécurité + Conformité + Vie privée + IA responsable

Découvrir les risques

Identifiez les données sensibles utilisées dans Copilot avec **Data Security Posture Management for AI**

Soyez alerté de l'utilisation risquée de Copilot avec **Communication Compliance**

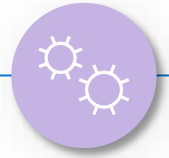
Détectez une séquence d'actions utilisateur à risque avec **Insider Risk Management**

Protéger les données

Détectez quand le contenu contient des données sensibles et appliquez des protections avec **Information Protection**

Bloquez l'accès de Copilot aux fichiers sensibles grâce à **Data Loss Prevention**

Ajustez automatiquement les politiques de sécurité en fonction du niveau de risque de l'utilisateur grâce à **la protection adaptative**



Gouverner l'utilisation

Interactions avec Audit Copilot et application des politiques de cycle de vie avec **Audit** et **Data Lifecycle Management**

Évaluez et suivez le respect des cadres réglementaires avec **Compliance Manager**

Inclure les interactions Copilot dans les enquêtes et les retentions légales avec **eDiscovery**

Microsoft Security